COBIT 5: ADDING VALUE THROUGH EFFECTIVE GEIT

DEREK OLIVER AND JOHN LAINHART

Abstract. The COBIT 5 framework is a significant evolution of the widely used COBIT 4.1. This article explores ISACA’s updated IT governance and management framework, and examines the business benefits of using COBIT 5. Readers will gain an understanding of the five principles of COBIT 5, and how the framework helps enterprises maximize the value of their information—the currency of the 21st century.

An orchestra is composed of many sections, with different instruments blending into one harmonious sound under the direction of a conductor. But imagine if the conductor managed only one portion of the instruments. Left to its devices, with no clear direction and defined responsibilities, the orchestra would likely be disastrous. Similarly, an enterprise’s information and technology must be managed and governed from end to end to achieve the most value from these critical assets. According to a study from the IT Governance Institute, enterprises that have implemented effective governance of enterprise IT (GEIT) report:

• Improved management of IT-related risk (42%)
• Improved communication and relationships between the business and IT (40%)
• Lower IT costs (38%)
• Improved IT delivery of business objectives (37%)
• Improved business competitiveness (28%)

COBIT 5, the newest version of ISACA’s flagship framework that was released on April 10, 2012, helps enterprises attain those benefits. COBIT 5 brings together broader business elements that make the framework applicable to the entire enterprise; it is no longer focused only on IT governance. COBIT 5 was also made simpler, with a foundation of just five principles using seven enablers, meaning that the core of the framework can be read and understood quickly.
COBIT 5 integrates ISACA frameworks such as Val IT and Risk IT. Additionally, it separates governance from management and focuses on board-level concerns, which makes it increasingly relevant to the business.

**THE EVOLUTION OF COBIT**

COBIT is now sixteen years old, and its roots are quite a bit older than that. It has evolved from its initial focus on information systems (IS) audit in 1996 through the stages listed below. Each version evolved to better meet the needs of the business to manage both its information and the most important medium supporting business information—information technology (IT).

- Prior to 1996, COBIT existed as the ISACA “Control Objectives” for IS auditors, which was issued as a loose-leaf manual to all ISACA Members (who, at the time, were primarily IS auditors)
- 1996—first framework was created primarily for auditors
- 1998—ISACA introduced control practices and control activities
- 2000—big change to include management guidelines and more
- 2005–2010—additional offerings including BMIS, Val IT, Risk IT
- 2012—COBIT 5

Many organizations throughout the world successfully used COBIT 4.1, but four main drivers helped influence the development of COBIT 5:

- A need to provide further guidance in areas with high interest, such as enterprise architecture, asset and service management, emerging sourcing, and enterprise models
- A need to provide further guidance in the area of innovation and emerging technologies; this is about creativity, inventiveness, developing new products, making the existing products more compelling to customers, and reaching new types of customers. Innovation also implies streamlining product development, manufacturing, and supply-chain processes to deliver products to market with increasing efficiency, speed, and quality
- A need to cover the full end-to-end business and IT functional responsibilities, and a need to cover all aspects that lead to effective governance and management of enterprise IT, such as...
organizational structures, policies, culture, and so on over and above processes
• A need to better govern and manage increasing user-initiated and user-controlled IT solutions

DIFFERENCES BETWEEN COBIT 5 AND COBIT 4.1

COBIT 5 has introduced five principles (see Figure 1) supported by seven enablers and a new set of processes that clearly separate governance from management. COBIT 5 also introduces a new process-reference model, new processes, updated and expanded goals and metrics, and alignment with the ISO/IEC 15504 process-capability-assessment model.

New Process Reference Model

The new processes in COBIT 5 include a brand new domain—Governance—which focuses the governance activities in a consistent way within COBIT 5. In COBIT 4.1, governance-related activities were interspersed among all processes and coordinated within a process (ME4).

Earlier versions of COBIT aligned with other frameworks and standards. COBIT 5 continues and enhances this approach, aligning with the latest frameworks and standards, enabling COBIT 5 to complement their use in enterprises, not compete with them.

As with earlier versions, it is important that users recognize COBIT 5 is a generic and customizable framework, to be used to

Figure 1  Five COBIT 5 principles. Source: ISACA, COBIT 5, 2012, figure 2, www.isaca.org/cobit. Used with permission.
match the existing process model of the enterprise to highlight any omissions or weaknesses.

New Processes

One of the goals of COBIT 5 is to align with the international standard ISO/IEC 38500 (governance). This led to the inclusion of the Evaluate, Direct, and Monitor (EDM) domain, which highlights the need for executive involvement in the governance of information. The EDM domain emphasizes that COBIT 5 is a business-wide document, not just for IT.

The revised processes have leveraged and improved on COBIT 4.1, Val IT, and Risk IT framework approaches. Many of these new and revised processes specifically relate to the expanded scope covered by Risk IT and Val IT.

As an example of a new process, the revised APO13 “Manage Security” does not reword the old DSS; COBIT 5 now differentiates security management from security operations, which are now DSS05.

The new processes in COBIT 5 are:

- APO03 Manage enterprise architecture
- APO04 Manage innovation
- APO05 Manage portfolio
- APO06 Manage budget and costs
- APO08 Manage relationships
- APO13 Manage security
- BAI05 Manage organizational change enablement
- BAI08 Manage knowledge
- BAI09 Manage assets
- DSS05 Manage security service
- DSS06 Manage business process controls

Goals and Metrics, Inputs and Outputs

Earlier versions of COBIT used a Goals Cascade and sample metrics, which were applied to address the detailed control objectives at the process level. COBIT 5 includes suggested metrics at the process goals level to evaluate the degree to which those goals are met.

It is important to emphasize a major difference between COBIT 4.1 and COBIT 5—the metrics in COBIT 4.1 were done at the process level, while the metrics in COBIT 5 are linked to specific process-related goals.

COBIT 5 does not depart from the concepts in 4.1 and continues to link stakeholder needs (based on the Kaplan-Norton balanced scorecard perspectives) to business goals to IT goals. It still includes suggested metrics at the higher level based on the enterprise goals that drive IT-related goals, and then are supported by critical processes.

COBIT 5 provides examples of goals and metrics at the enterprise, process, and management-practice levels. This is a change from COBIT 4.1, Val IT, and Risk IT, which went down one level lower.

As an explanation, COBIT 4.1 included references to the origin and destination of inputs and outputs at the process level. COBIT 5
now provides these references at the governance—or management-practice—level.

This is a useful addition when implementing or transitioning, as users can ensure the outputs from each governance or management practice reach their designated targets. Also, it provides additional detailed guidance for designing processes to include essential work products and to assist with interprocess integration.

COBIT 4.1, Val IT, and Risk IT provided RACI (Responsible, Accountable, Consulted, Informed) charts, but those in COBIT 5 are considerably more detailed. The COBIT 5 RACI charts are color-coded to distinguish between business and IT roles.

COBIT 5 PRINCIPLES

The core of COBIT 5 is its five basic principles, which can be used together with the seven categories of enablers to govern and manage the information requirements of the enterprise.

The five principles are:

1. Meeting stakeholder needs
2. Covering the enterprise end-to-end
3. Applying a single, integrated framework
4. Enabling a holistic approach
5. Separating governance from management

Principle 1: Meeting Stakeholder Needs

There is one word that links all stakeholder needs: value. Everyone—customer, shareholder, executive, line manager, member, or voter—expects to get value for money or for effort. The nature of the stakeholder will often determine the meaning of the word value, whether it be financial, service levels, accuracy, completeness, or confidentiality.

Benefits can take many forms and shapes. For example, benefits are financial for commercial enterprises, while benefits are service for government agencies. Creating value means realizing benefits at an optimal resource cost while optimizing risk. “Creating value” means different (and sometimes conflicting) things to each stakeholder in an enterprise, and enterprises may have many stakeholders.

Governance is about negotiating, deciding among different stakeholders’ value interests, and considering all stakeholders when making benefit, resource, and risk assessment decisions. Governance evaluates, directs, and monitors. At the highest level, executives must identify who all of the enterprise stakeholders are and what their needs are, and then establish the hierarchy.

At the management levels, each manager must identify relevant stakeholders and identify what has to be done to address their needs.

At each level, the following questions must be addressed:

- Who are the benefits for?
- Who bears the risk?
- What resources are required?
Meeting stakeholder needs is supported by the COBIT 5 Goals Cascade, which translates stakeholder needs into specific, practical, and customized goals within the context of the enterprise, IT-related goals, and enabler goals.

The new COBIT 5 Goals Cascade helps to ensure the top-down approach to GEIT by starting from the stakeholder drivers and needs. It defines relevant and tangible goals and objectives at various levels of responsibility. It also filters the knowledge base of COBIT 5, based on enterprise goals, to extract relevant guidance for inclusion in specific implementation, improvement, or assurance projects. It clearly identifies and communicates how enablers are used to achieve enterprise goals. Note that COBIT 5 does not focus entirely on technology but also the need to manage information across the enterprise to meet the particular needs of individual stakeholders.

COBIT 5 integrates GEIT into enterprise governance—that is, the governance system for enterprise IT proposed by COBIT 5 integrates seamlessly into any governance system. COBIT 5 also covers all information- and technology-related functions and processes within the enterprise.

COBIT 5 does not focus on the IT function, but treats information and related technologies as assets that need to be dealt with just like any other asset within the enterprise.

**Principle 2: Covering the Enterprise End-to-End**

The foundation of COBIT 5 is the end-to-end governance of the enterprise, and the objective of governance is value creation.

**Governance enablers**

Governance enablers are the organizational resources for governance (frameworks, principles, structure, processes, practices) toward which or through which action is directed and objectives can be attained. Enablers also include the enterprise’s resources—service capabilities such as IT infrastructure, IT applications, people, and information.

A lack of resources or enablers may affect the ability of the enterprise to create value. Given the importance of governance enablers, COBIT 5 includes a single way of looking at and working with enablers.

**Governance scope**

Governance can be applied to the whole enterprise, an entity, a tangible or intangible asset, and so on. This makes it possible to define different views of the enterprise to which governance is applied. It is essential to define this scope of the governance system well.

The scope of the COBIT 5 Process Reference Model is a function view—the function being IT or information and related technologies across the enterprise.
Governance roles, activities, and relationships

Governance roles, activities, and relationships define who is involved in governance, how they are involved, what they do, and how they interact within the scope of any governance system.

In COBIT 5, a clear differentiation is made between governance and management practices in the governance and management domains, as well as how they interface with the role players that are involved.

Principle 3—Applying a Single Integrated Framework

COBIT 5 aligns with the latest relevant standards and frameworks, allowing an enterprise to use COBIT 5 as its overarching governance and management framework. It also offers complete enterprise coverage, providing a basis to integrate effectively with the other frameworks, standards, and practices used.

COBIT 5 integrates all knowledge previously dispersed over different ISACA frameworks. ISACA has researched the key area of enterprise governance for many years and has developed frameworks such as COBIT, Val IT, Risk IT, Board Briefing on IT Governance, the Business Model for Information Security (BMIS), and the IT Assurance Framework (ITAF) to provide guidance and assistance to enterprises.

COBIT 5 provides a simple architecture for structuring guidance materials and producing a consistent product set. The COBIT 5 product family (the current, under-development, and proposed products) allows users to focus on their precise needs, whether they be security, assurance, risk management, and so on, with ongoing direction to other frameworks or standards external to ISACA. A collaborative online environment will also be made available to support the use of COBIT 5.

Principle 4—Enabling a Holistic Approach

The COBIT 5 enablers, driven by the Goals Cascade, are factors that, individually and collectively, influence whether something will work. The higher-level, IT-related goals define what the different enablers should achieve, while the Goals Cascade links stakeholder needs to the enablers. The mapping table between IT-related goals and enterprise goals is included in COBIT 5, Appendix B, showing how each enterprise goal is supported by a number of IT-related goals.

The COBIT 5 Goals Cascade:

- Links stakeholder needs to enterprise goals
- Links enterprise goals to IT goals
- Connects the IT goals to the enablers

Achieving IT-related goals requires the successful application and use of seven enablers. It is important to note that principles, policies, and frameworks are in the center (see Figure 2), linking the other six enablers to show that they are the foundation for all governance and management activities.
COBIT 5 enablers include:

1. **Principles, policies and frameworks**—the vehicle to translate the desired behavior into practical guidance for day-to-day management
2. **Processes**—organized set of practices and activities to achieve objectives and produce a set of outputs in support of achieving overall IT-related goals
3. **Organizational structures**—the key decision-making entities in an enterprise
4. **Culture, ethics, and behavior**—of individuals and of the enterprise; very often underestimated as a success factor in governance and management activities
5. **Information**—pervasive throughout any enterprise (i.e., deals with all information produced and used by the enterprise). Information is required for keeping the enterprise running and well-governed, but at the operational level, information is very often the key product of the enterprise itself
6. **Services, infrastructure, and applications**—the infrastructure, technology, and applications that provide the enterprise with information-technology processing and services
7. **People, skills, and competences**—required for successful completion of all activities and for making correct decisions and taking corrective actions

All enablers have a set of common dimensions that provide a common, simple, and structured way to deal with them, while enabling an entity to manage its complex interactions and facilitate successful outcomes of the enablers.

The four common dimensions for enablers are:

- **Stakeholders**—parties who play an active role and/or have an interest in the enabler (e.g., processes have different parties who execute process activities and/or who have an interest in the process outcomes):
Organizational structures have stakeholders, each with their own roles and interests.

- Stakeholders can be internal or external to the enterprise, all having their own (sometimes conflicting) interests and needs.
- Stakeholders' needs translate to enterprise goals, which in turn translate to IT-related goals for the enterprise.

**Goals**—expected outcomes:

- Enablers provide value by the achievement of these goals. The enabler goals are the final step in the COBIT 5 Goals Cascade.
- Goals can be further split up in different categories:
  - **Intrinsic Quality**—the extent to which enablers provide accurate, objective, and reputable results.
  - **Contextual Quality**—the extent to which outcomes of the enabler are fit for purpose given the context in which they operate (e.g., outcomes should be relevant, complete, current, appropriate, consistent, understandable, and easy to use).
  - **Access and Security**—the extent to which enablers are accessible and available when needed and secured.

**Lifecycle**—each enabler has a lifecycle, from inception through an operational/useful life until disposal. This applies to information, structures, processes, policies, and so on. The phases of the lifecycle consist of:

- Plan
- Design
- Build/Acquire/Create/Implement
- Use/Operate
- Evaluate/Monitor
- Update/Dispose

**Good practices**—support the achievement of the enabler goals. Good practices provide examples on how to best implement the enabler, and what work products (or inputs and outputs) are required. COBIT 5 offers examples of good practices for the enablers provided by COBIT 5 (e.g., Processes). For other enablers, guidance from other standards or frameworks can be used.

**Principle 5—Separating Governance From Management**

The COBIT 5 framework makes a clear distinction between governance and management. In most enterprises, the major governance activities are the responsibility of the board of directors under the leadership of the chairperson, while most management activities are the responsibility of the executive management under the leadership of the CEO.

In COBIT 5:

- Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives (EDM).
- Management plans, builds, runs, and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).

These definitions apply particularly to the differences in implementing and maintaining good information governance in an enterprise. The COBIT 5: Enabling Processes guide differentiates the activities associated with each. The process model has a new domain specifically related to governance activities.

COBIT 5 advocates that enterprises implement governance and management processes to ensure key areas are covered. An enterprise can organize its processes as it sees fit, as long as all necessary governance and management objectives are covered. Smaller enterprises may have fewer processes; larger and more complex enterprises may have many processes, all to cover the same objectives.

COBIT 5 includes a process reference model, which defines and describes in detail a number of governance and management processes. It represents all the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT and business managers.

The proposed process model is a complete, comprehensive model, but it is not the only possible process model. Each enterprise must define its own process set, taking into account its specific situation.

**COBIT 5 PROCESS CAPABILITY MODEL: A MAJOR IMPROVEMENT**

The new COBIT 5 Process Capability Model improves on the previous CMM-based Maturity Model; it is based on the ISO/IEC 15504 Software Engineering–Process Assessment standard. The differences between the two models and the benefits of the COBIT 5 approach, as well as some practical usage examples, are included in the new COBIT Assessment Programme publications, which explain the difference between the CMM and the new ISO 15504 approaches, summarize the differences COBIT users will encounter in practice, and guide users on performing a COBIT process-based capability assessment.

The new approach is not a maturity assessment (which is performed at the enterprise level in ISO/IEC 15504). Rather, it is a process-capability assessment at the process level only.

The new approach is more robust, reliable, and repeatable and supported by an international standard. It is being used especially by financial institutions in Europe to complement existing audits on internal controls by providing a lens on process capability with a view to assessing what processes need to be improved.

Assessments done using the old COBIT 4.1 CMM approach cannot be translated to the new approach. COBIT 4.1, Val IT and Risk IT users may continue with the CMM-based approach using COBIT 4.1. Users are encouraged, however, to adopt the new approach.
In addition to the COBIT 5 framework itself, ISACA also issued an updated version of its IT governance implementation document, now called COBIT 5 Implementation, to support COBIT users with either (1) their transition from version 4 to 5 or (2) implementation of GEIT arrangements from scratch. The approach taken by this guide is that of a quality improvement cycle, portrayed in Figure 3.

WHY USE COBIT 5?

According to a blog post from ITPolicyCompliance.com, “If you’re interested in maximizing the most value and minimizing risks related to the use of IT, then COBIT 5 should be important to you. The best-in-class organizations already understand this.”

COBIT 5 was created to directly address business needs, and it cross-references to all relevant, internationally recognized standards and frameworks (e.g., ITIL, TOGAF, PMBOK, PRINCE2, COSO, and ISO standards). In driving effective GEIT through the use of COBIT 5, enterprises are likely to realize the following benefits:

- Better value creation through effective and innovative use of enterprise IT
- Increased business-user satisfaction with IT engagement and services
- Increased compliance with relevant laws, regulations, and policies
- Improved relationship between business needs and IT objectives
- Increased financial return from GEIT by obtaining the greatest value from investments in technology

The COBIT 5 family of products currently consists of:

- COBIT 5 (the framework)
- COBIT 5 Implementation
• COBIT 5: Enabling Processes
• COBIT 5 for Information Security

Additional guides, including COBIT 5: Enabling Information, COBIT 5 for Risk, and COBIT 5 for Assurance, will be available in the future. The first four publications can be downloaded at www.isaca.org/cobit. The framework publication is available free of charge.

Information has become the currency of the 21st century. From the time that information is created to the moment that it is destroyed, technology plays a significant role across the enterprise. By approaching IT governance from a business perspective, COBIT 5 helps enterprises maximize the trust in, and value from, their information and technology.

Note

ACKNOWLEDGMENT
 Portions of this article were excerpted from COBIT 5 with permission from ISACA.

Derek Oliver and John Lainhart were cochairs of the COBIT 5 Task Force and are members of ISACA’s Framework Committee.